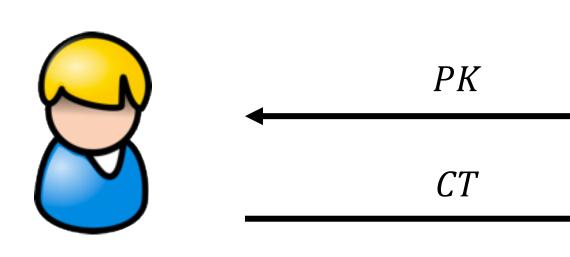
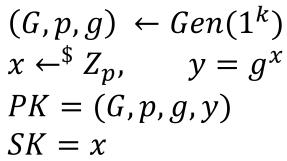
## ElGamal Encryption 과제

## ElGamal Encryption







$$Enc_{PK}(m)$$
:  
 $r \leftarrow^{\$} Z_p$   
 $CT = \langle g^r, m \cdot y^r \rangle$ 

$$Dec_{SK}(CT):$$

$$C1, C2 \leftarrow CT$$

$$m = \frac{C2}{C1^{x}}$$

```
Setup:
        p ← random 1024 bit safe prime
        g (p의 generator)
       x \leftarrow Z_{p}
        y = g^x \mod p
        pub = (p,q,y)
        priv = x
Enc(m, pub):
       r \leftarrow Z_p
       c_1 = g^r \mod p
       c_2 = m \cdot y^r \mod p
Dec(C, priv, pub) :
       C = (c_1, c_2)
       m = \frac{c_2}{c_1^x} \mod p
```

## 출력 예:

```
Complete the select of safe prime
Complete the select of generator
p : D5ED6D8C3A0192340D253236F3AB15C3472
D2D777AD16ADD4C768C5962C782A5415D064B07FD2F82
g : 05
c1 : A184EEDDB9C59F6AD1E968F81C39D63D0018AC96E2F337F559AB2A3C13FE3607A9F3B76261D403F82
c2 : 56DD982EC04F4F51A29607BC948A49A3C916A6894DB4E58F686561353D70C972DB03490ED1779E63
dec : hello
msg_len : 5
```

※실행이 수 초간 소요될 수 있음

<-  $c_2$ 와  $c_1^x$ 의 inverse(mod p 에 대한) 를 곱하면 됩니다. =  $c_2$  \* inv( $c_1^x$ ) mod p